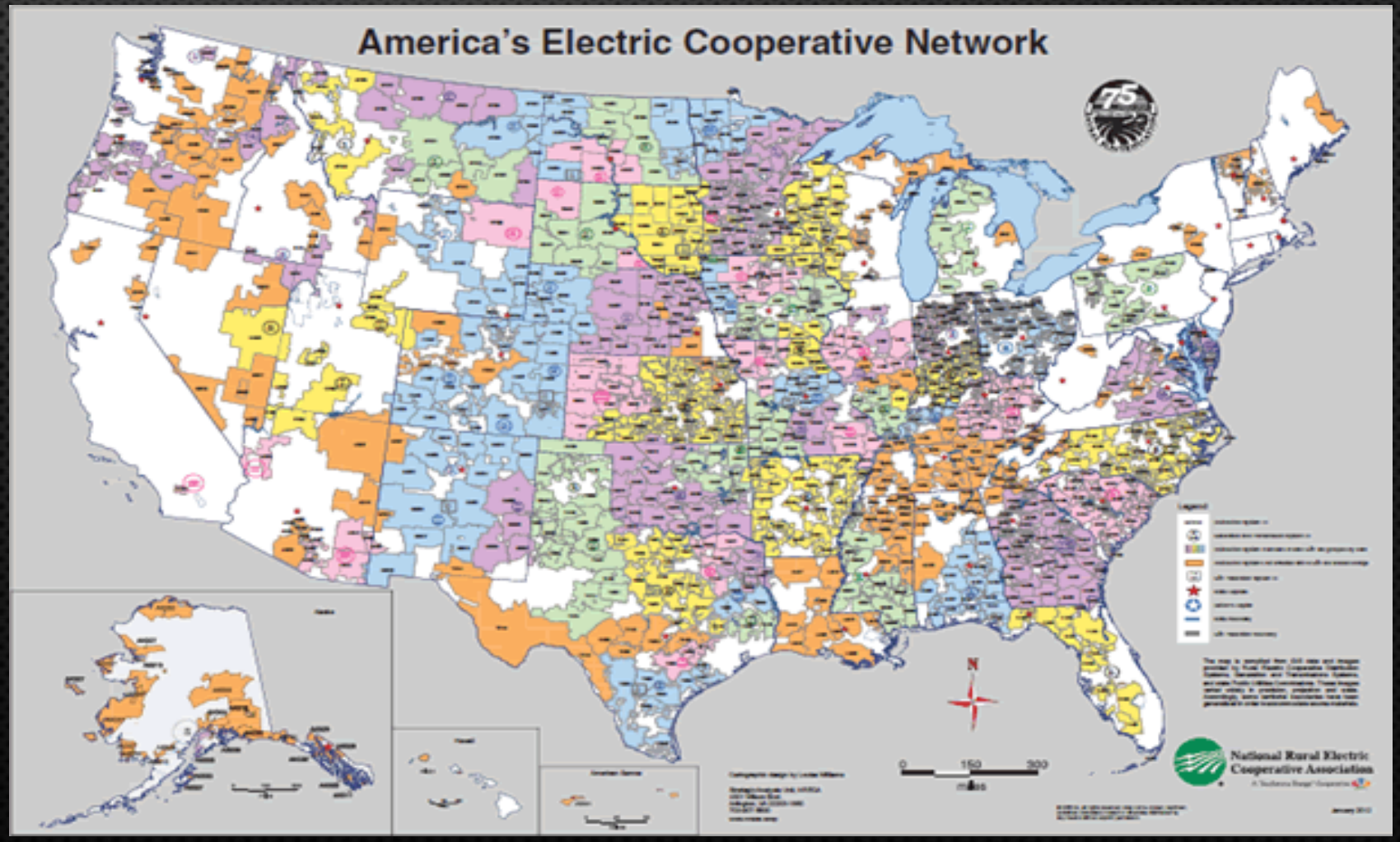
BUILDING RESILIENT CYBER SYSTEMS

Cynthia Hsu

National Rural Electric Cooperative association

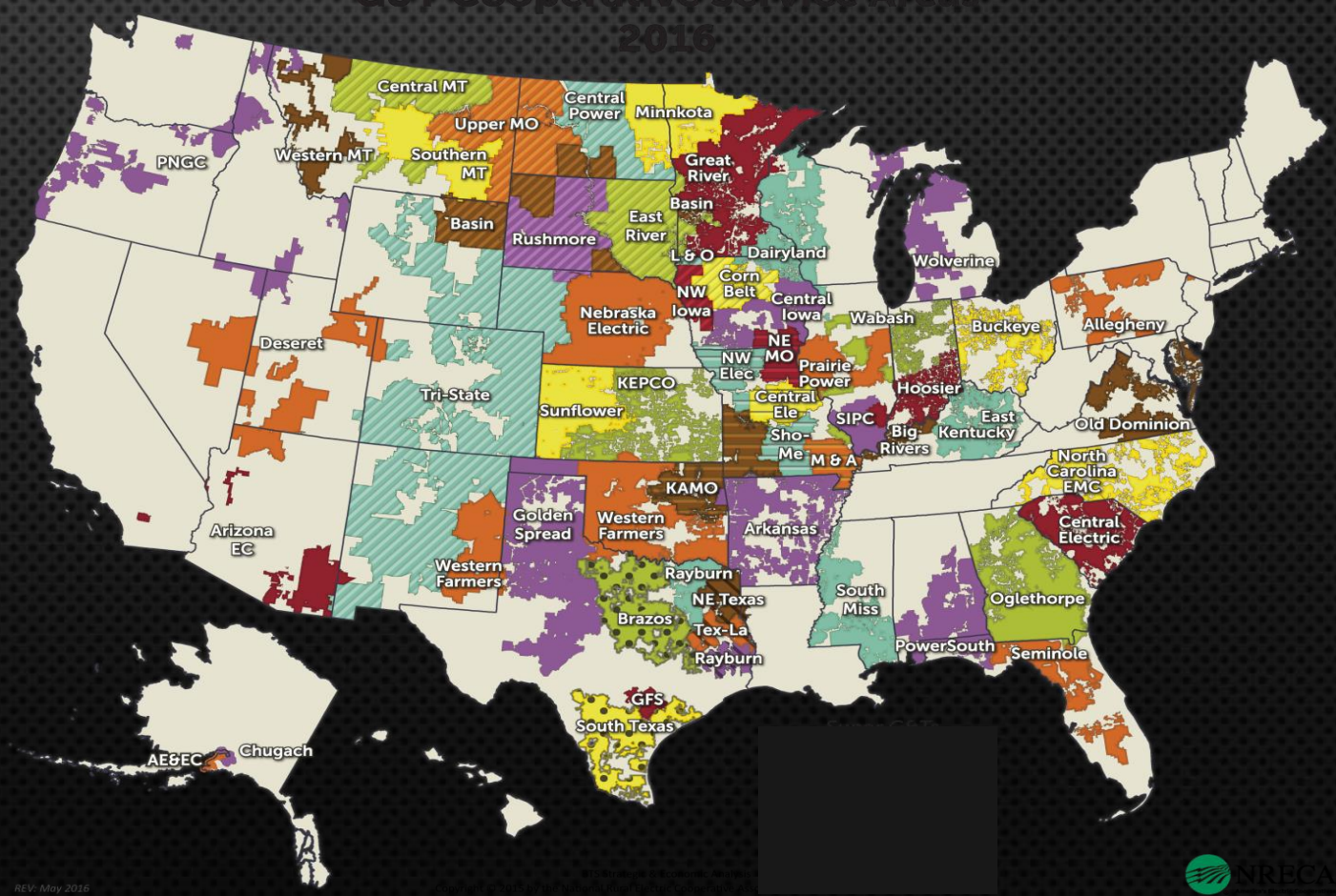
WHAT ARE THE CO-OPS? WHO IS NRECA?

- 900+ Co-ops
- 75% of the US Land Mass
- 42 million people in 47 states
- 18 million commercial accounts
- Much lower density
- Higher levels of smart grid technology
- Co-operative technology



WHAT ARE THE CO-OPS?
WHO IS NRECA?

- 66 Generation and Transmission Cooperatives
- 55,000 MW capacity
- 5% of the U.S.

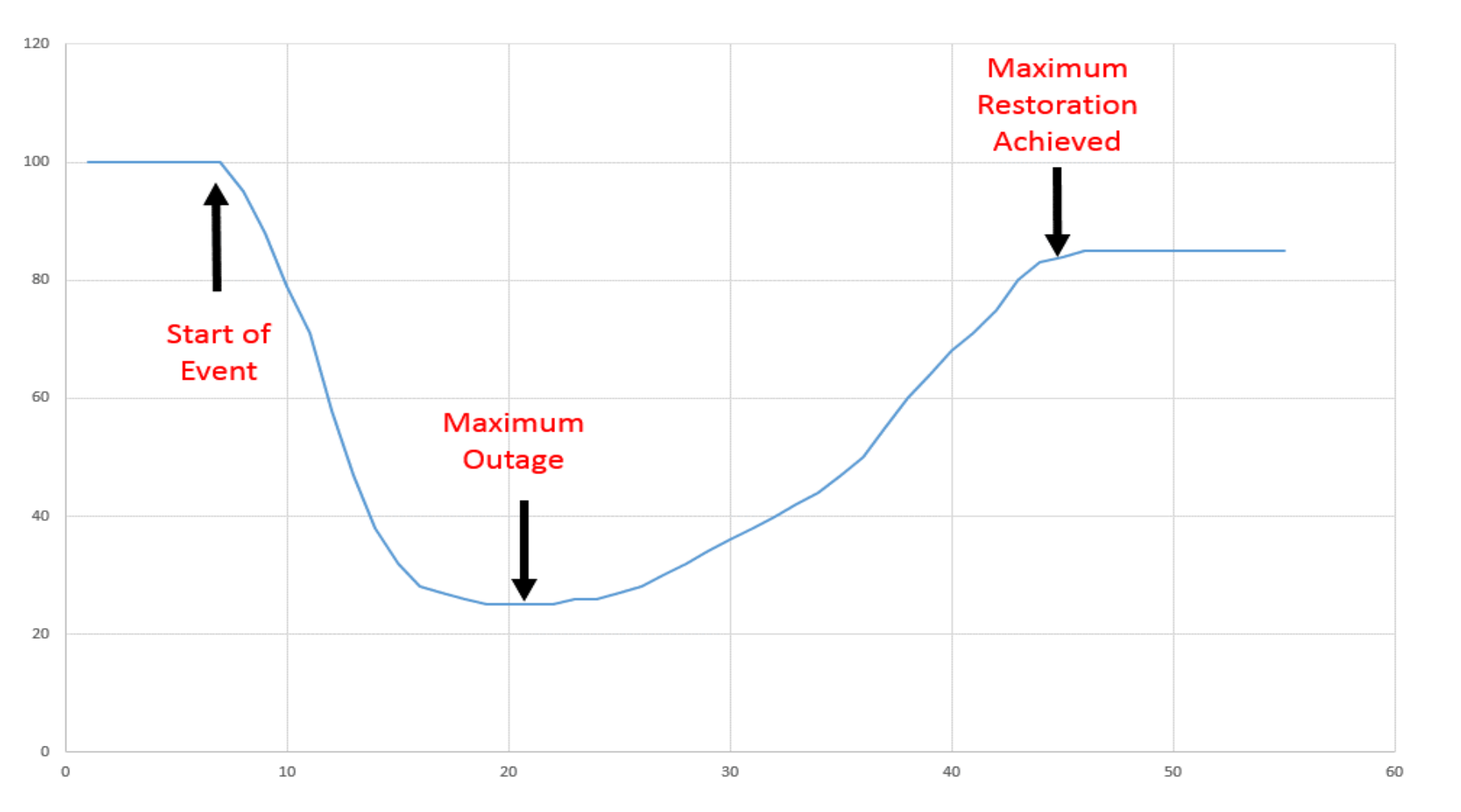


RESILIENCY

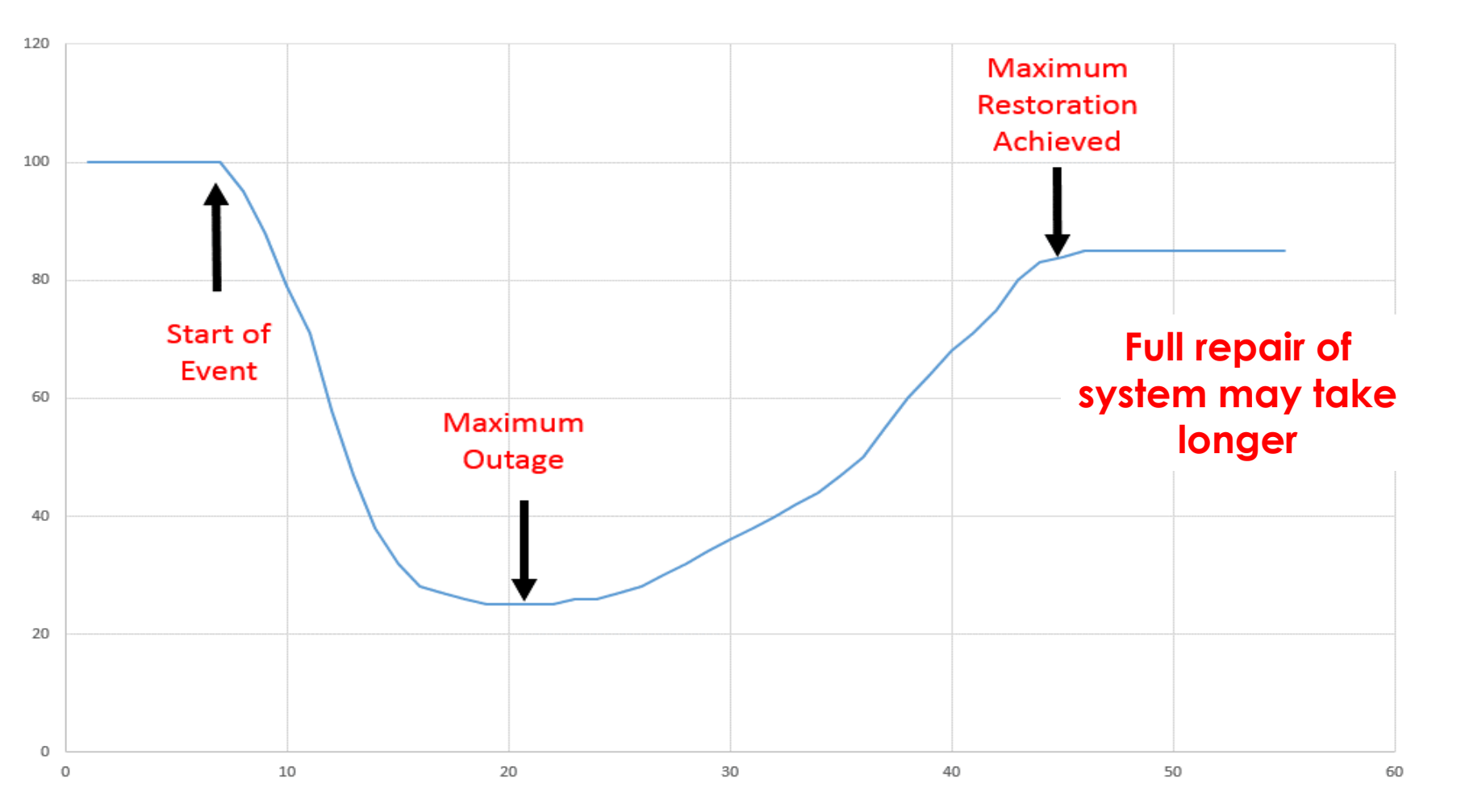
"The ability to maintain or recover normal or near-normal service or status of the system through planning, prevention, mitigation, response and recovery efforts."

NRECA
America's Electric Cooperatives

TIME LINE OF A DISASTER

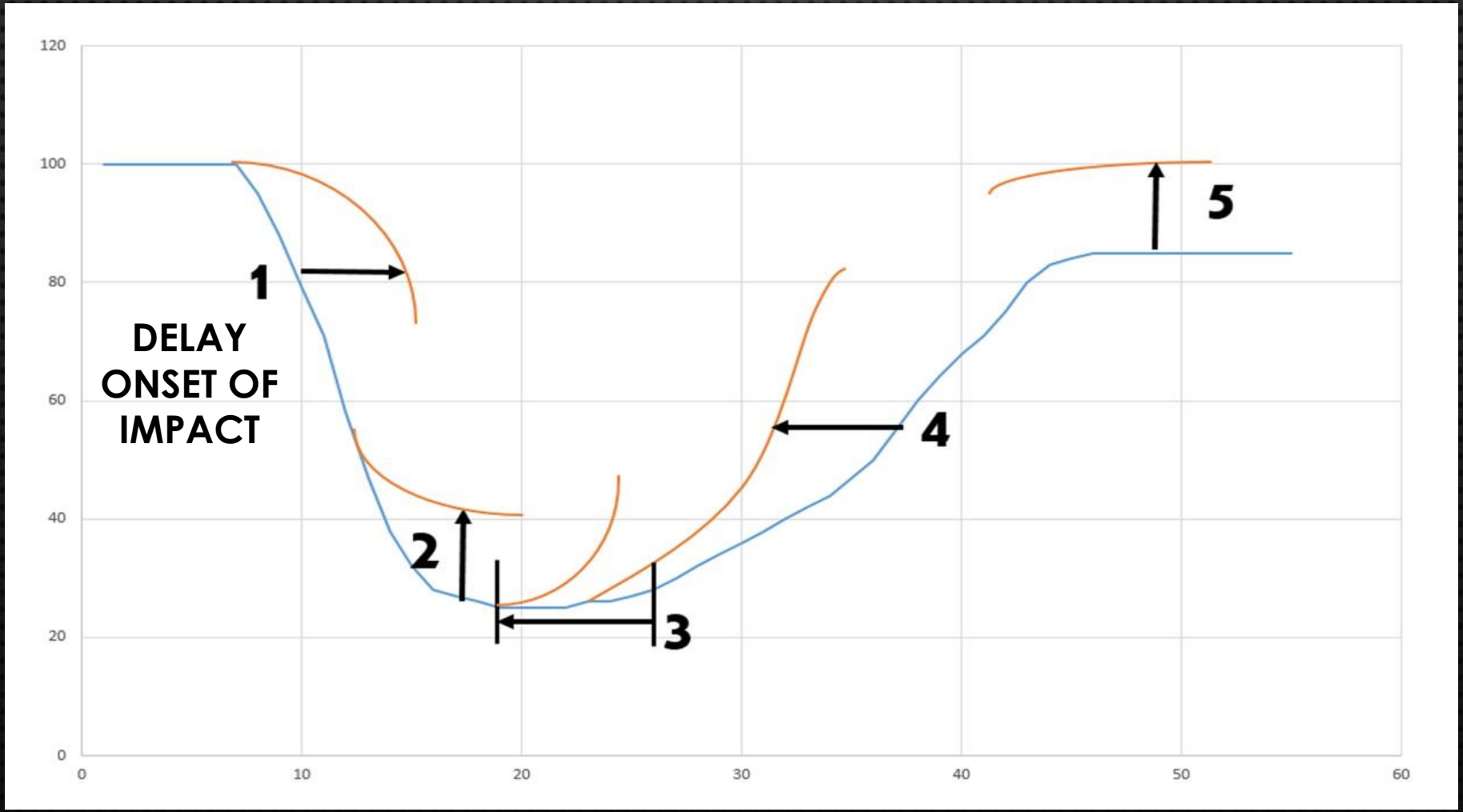


TIME LINE OF A DISASTER

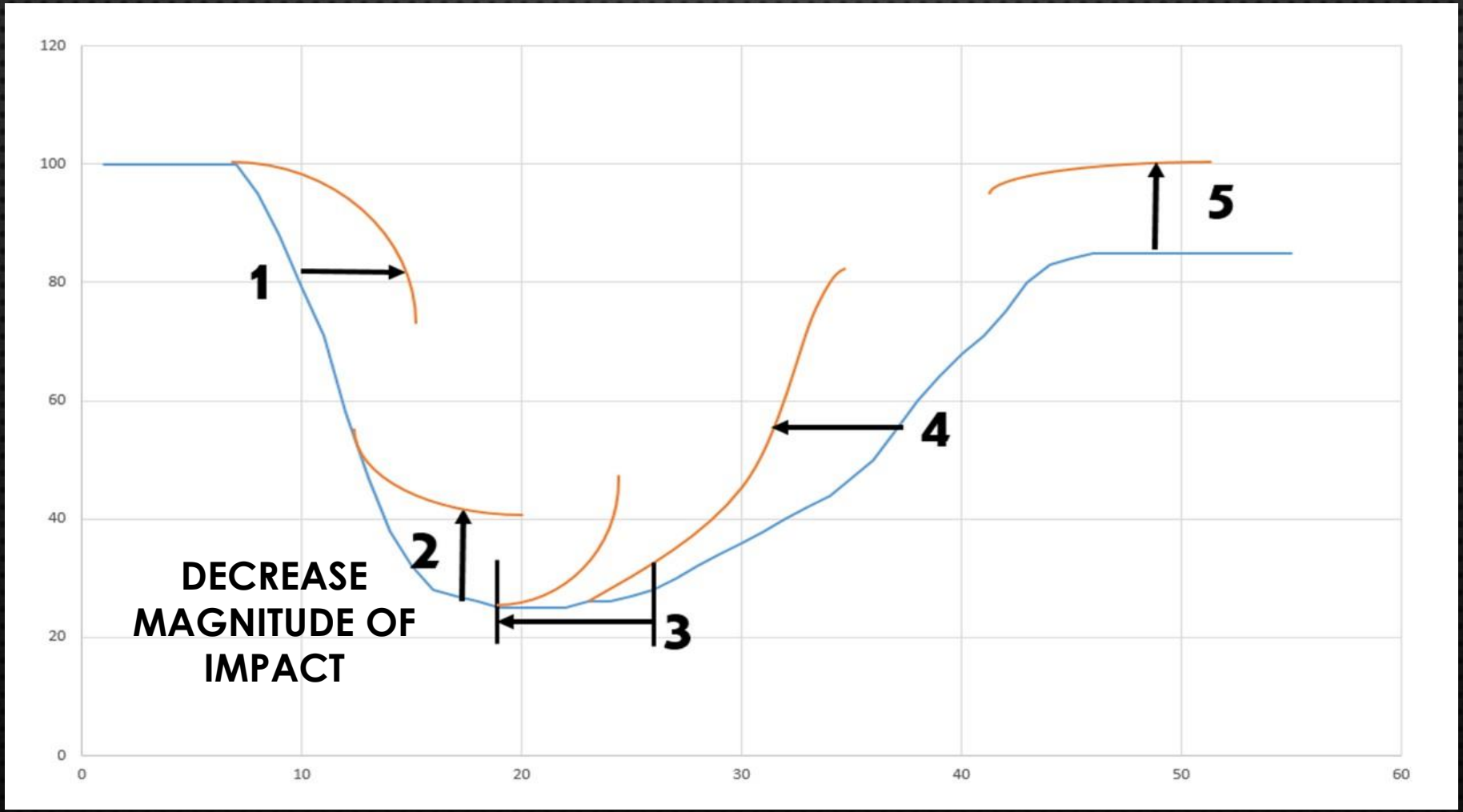


How can we do better?

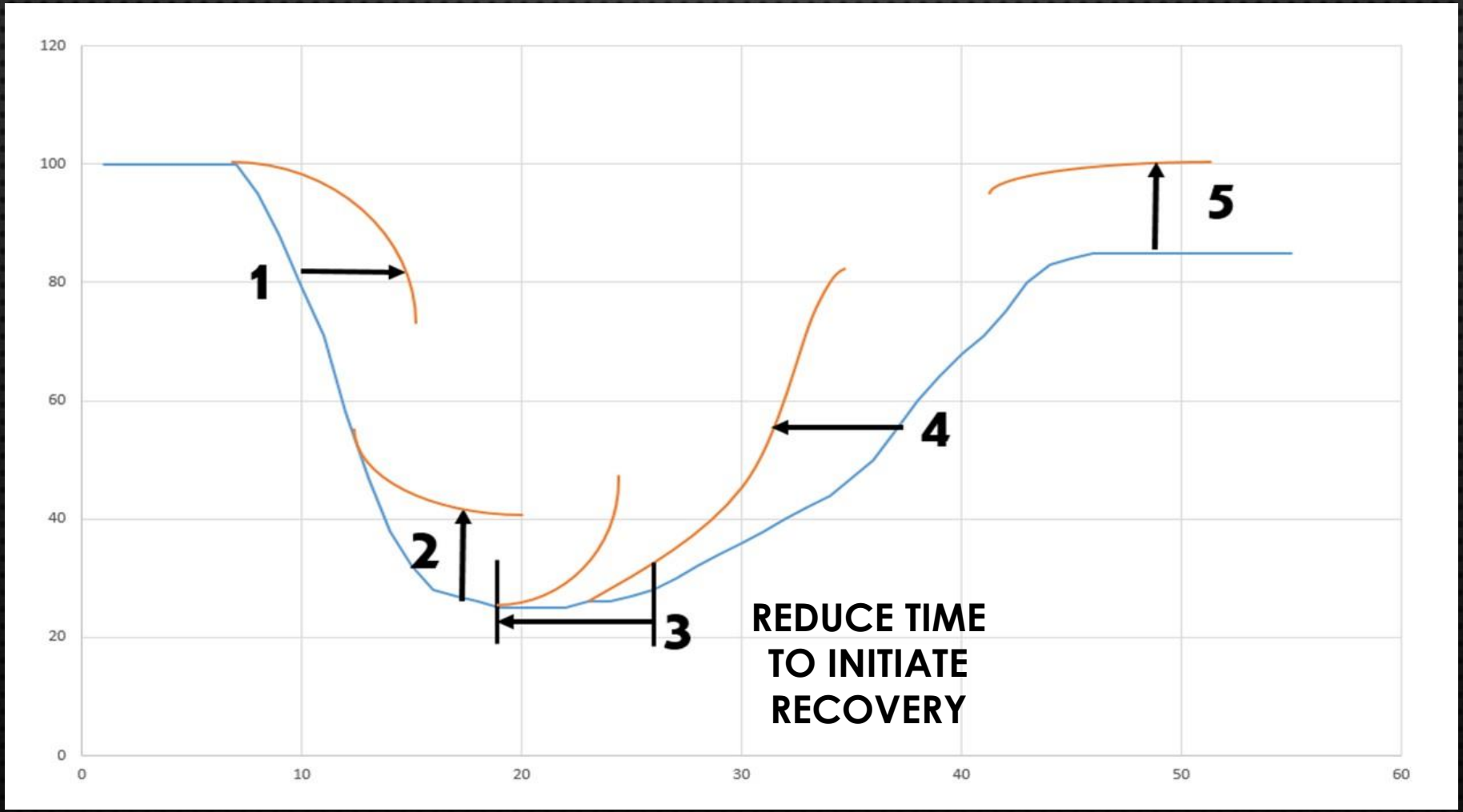
HOW CAN WE DO BETTER?



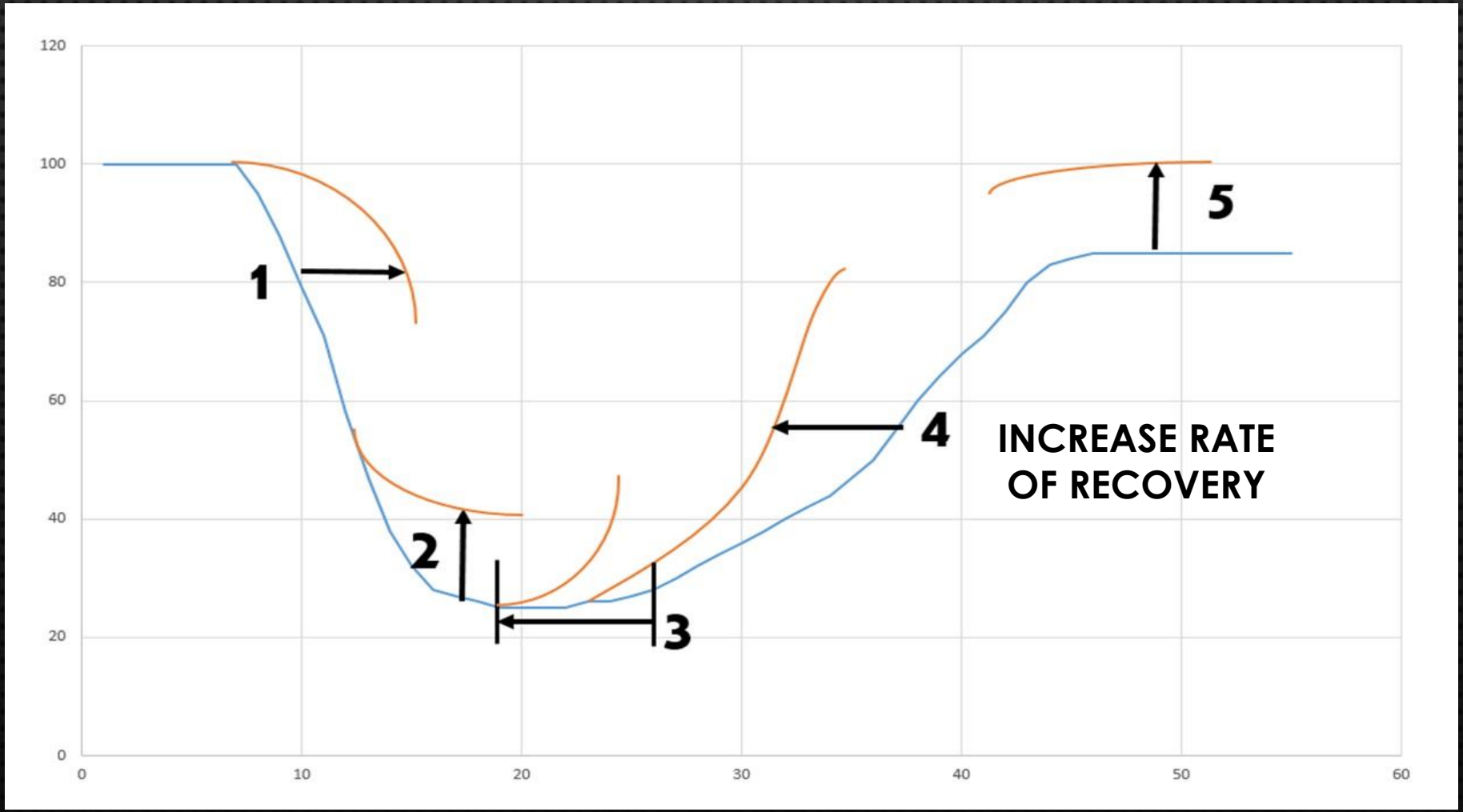
HOW CAN WE DO BETTER?



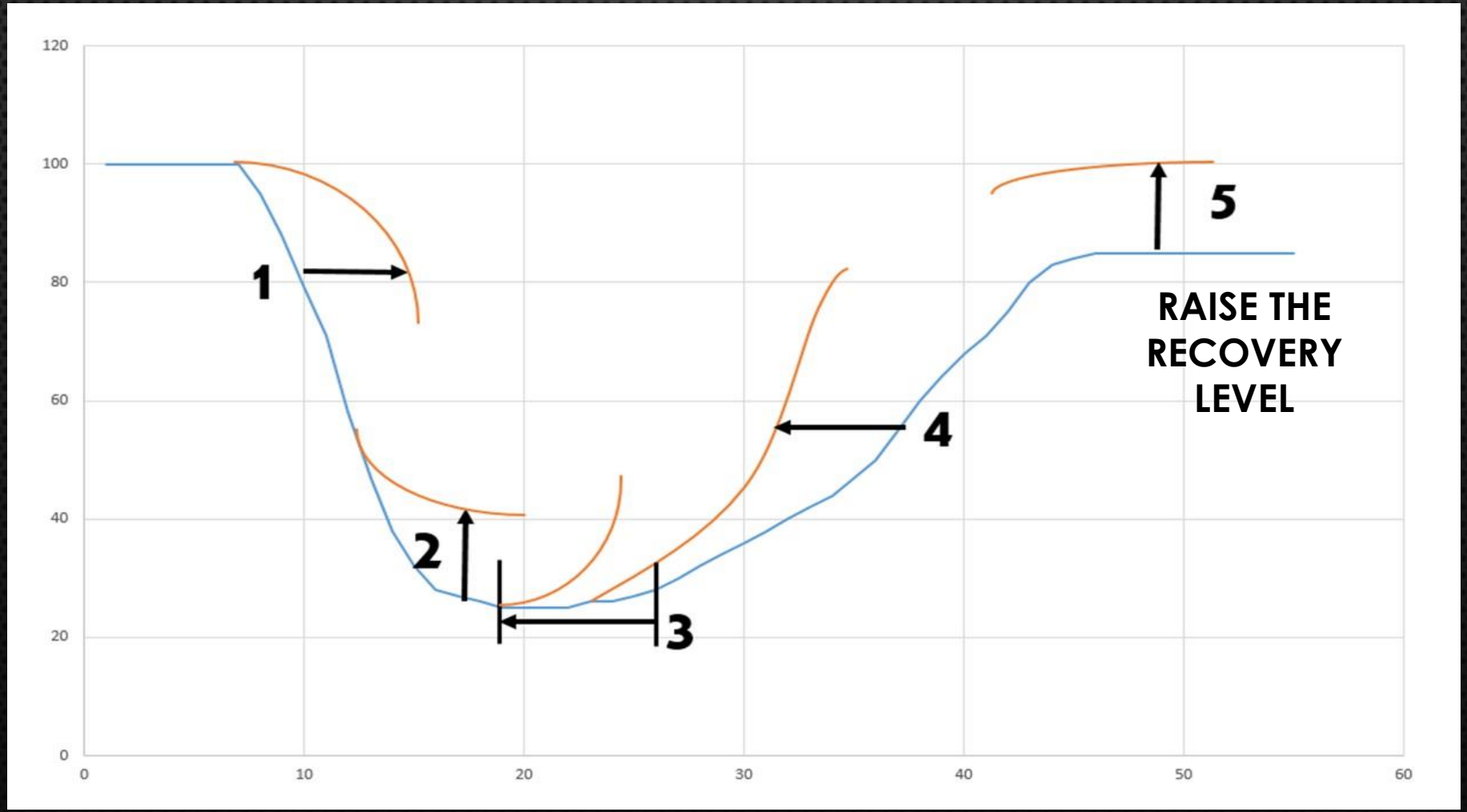
HOW CAN WE DO BETTER?



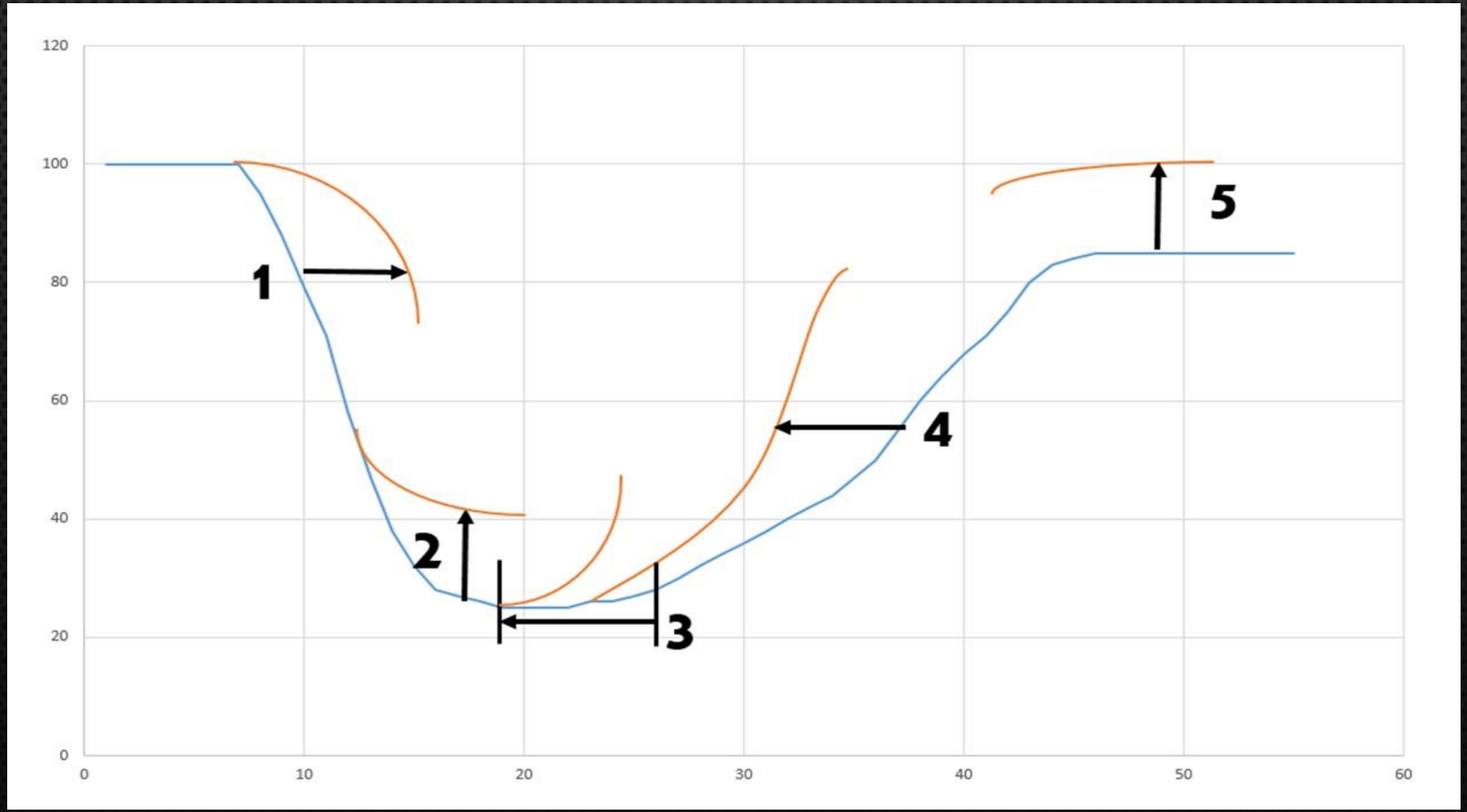
HOW CAN WE DO BETTER?



HOW CAN WE DO BETTER?

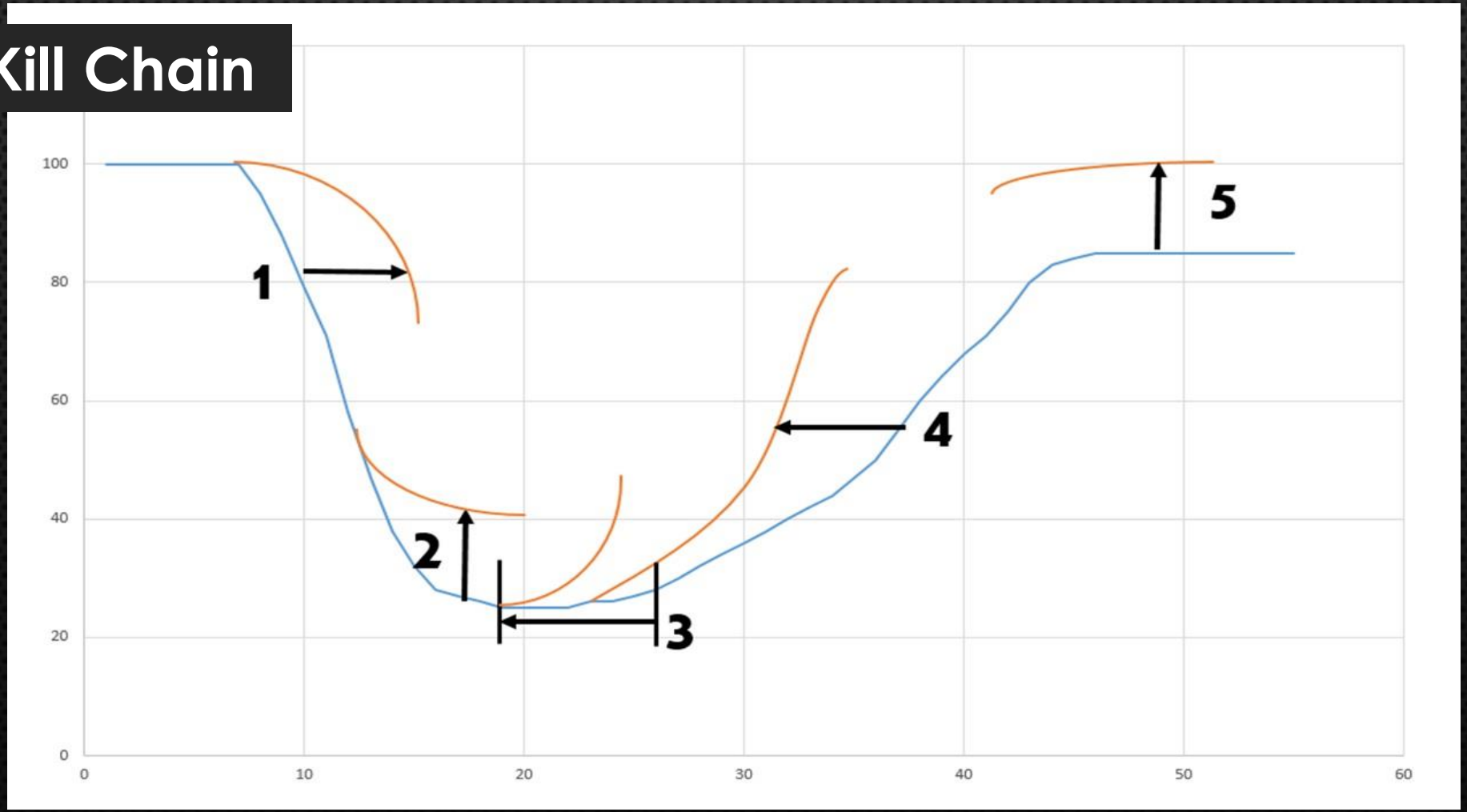


CAN THIS MODEL BE APPLIED TO CYBER?



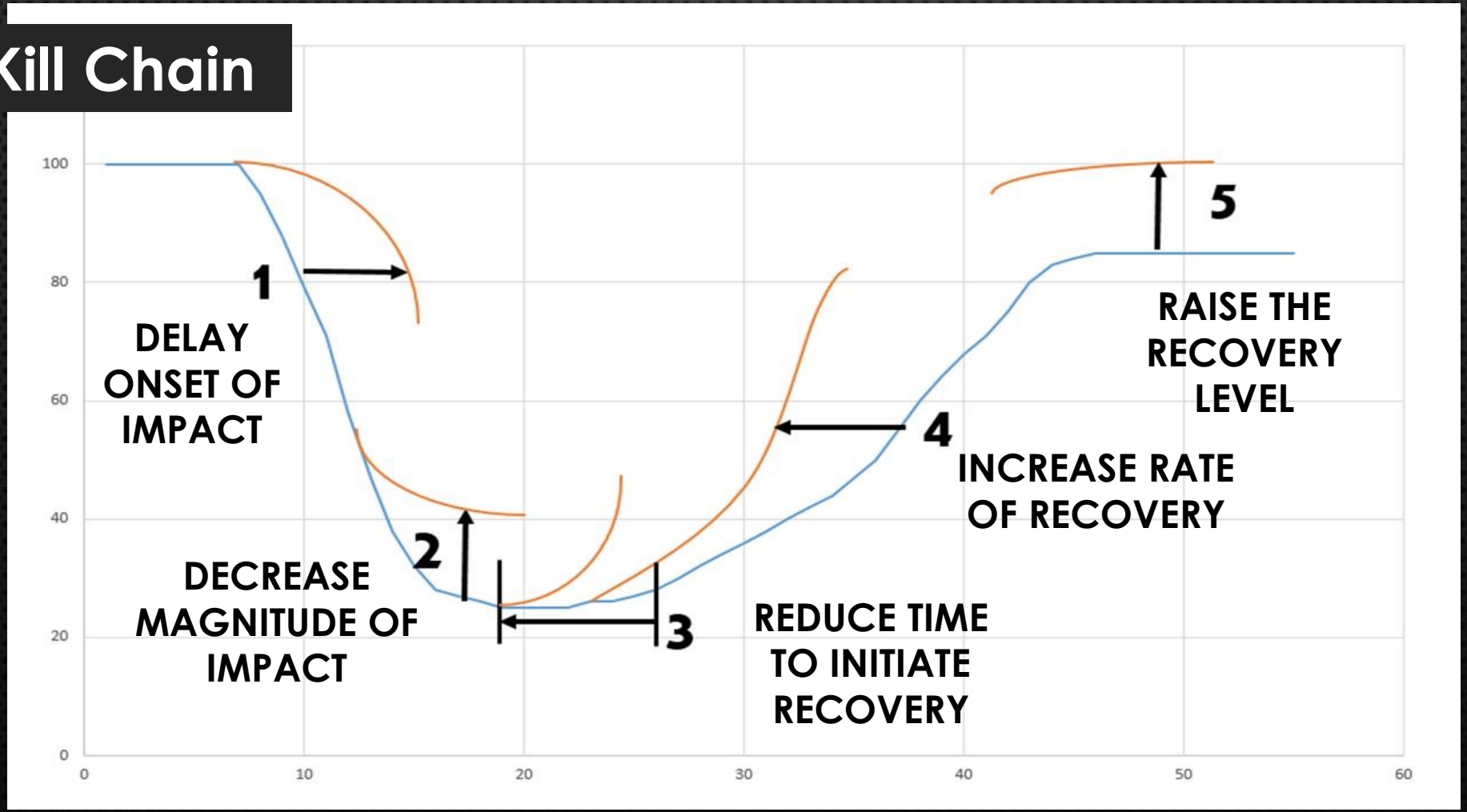
CAN THIS MODEL BE APPLIED TO CYBER?

ICS Kill Chain



2-5 → R&D still needed

ICS Kill Chain



NIST Framework

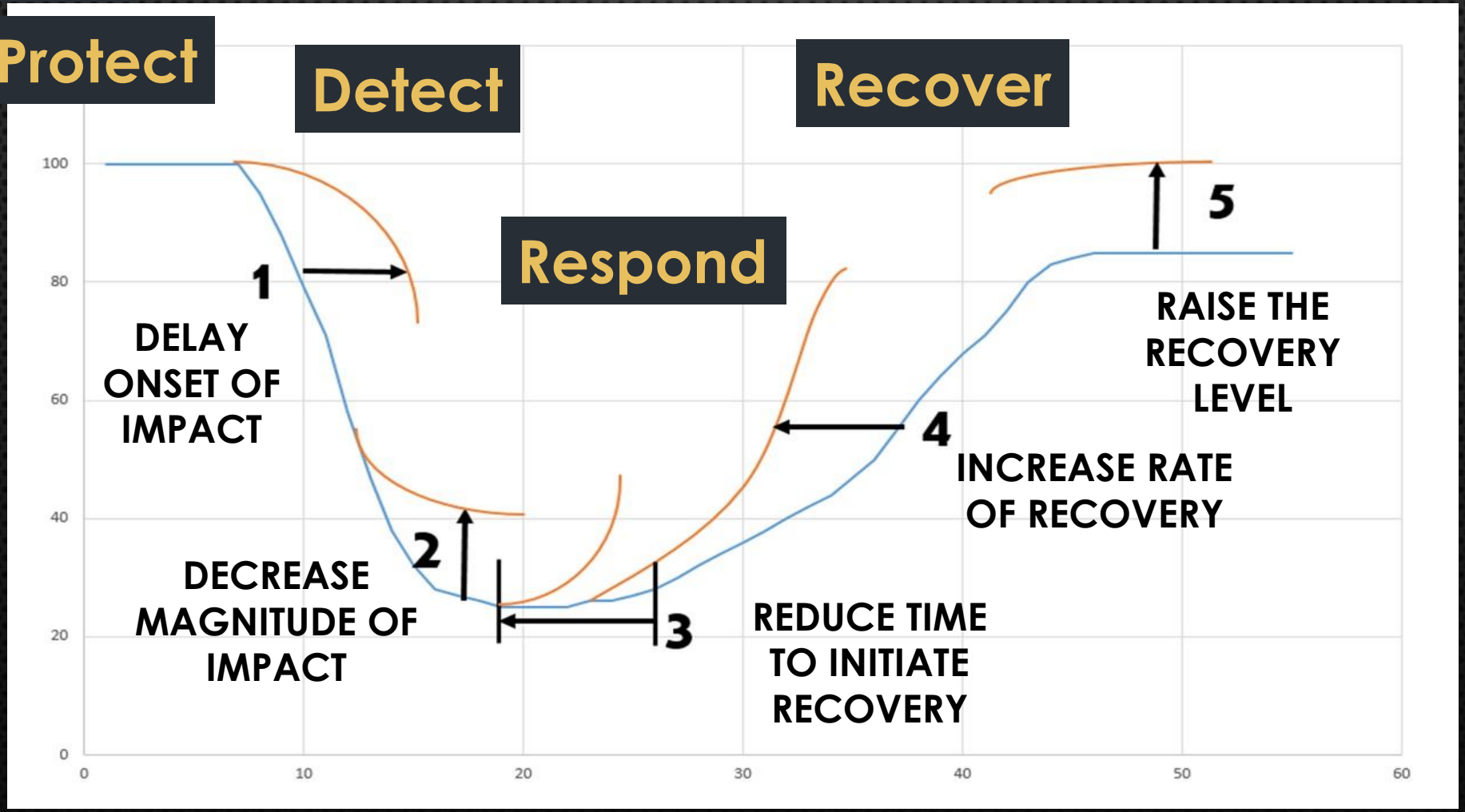
Identify

Protect

Detect

Recover

Respond



25 Research Programs – "cyber"

1. Active Authentication
2. Active Cyber Defense (ACD)
3. Automated Program Analysis for Cybersecurity (APAC)
4. Behavioral Learning for Adaptive Electronic Warfare (BLADE)
5. Building Resource Adaptive Software Systems (BRASS)
6. Clean-slate design of Resilience, Adaptive, Secure Hosts (CRASH)
7. Computer Science Study Group (CSSG)
8. Crowd Sourced Formal Verification (CSFV)
9. Cyber Fault-tolerant Attack Recovery (CFAR)
10. Cyber Grand Challenge (CGC)
11. Dispersed Computing
12. Edge-Directed Cyber Technologies for Reliable Mission Communication (Edge CT)
13. Enhanced Attribution
14. Extreme DDoS Defense (XD3)
15. High-Assurance Cyber Military Systems (HACMS)
16. Integrated Cyber Analysis System (ICAS)
17. Leveraging the Analog Domain for Security (LADS)
18. Memex
19. Mission-oriented Resilient Clouds (MRC)
20. Plan X
21. Rapid Attack Detection, Isolation and Characterization Systems (RADICS)
22. Safeware
23. Space/Time Analysis for Cybersecurity (STAC)
24. Transparent Computing
25. Vetting Commodity IT Software and Firmware (VET)

DEFENSE ADVANCED
RESEARCH PROJECTS AGENCY

Building Resource Adaptive Software Systems (BRASS)

Dr. Suresh Jagannathan

DEFENSE ADVANCED
RESEARCH PROJECTS AGENCY

Building Resource Adaptive Software Systems (BRASS)

Dr. Suresh Jagannathan

Modern-day software operates within a complex ecosystem of libraries, models, protocols and devices. Ecosystems change over time in response to new technologies or paradigms, as a consequence of repairing discovered vulnerabilities (security, logical, or performance-related), or because of varying resource availability and reconfiguration of the underlying execution platform. When these changes occur, applications may no longer work as expected because their assumptions on how the ecosystem should behave may have been inadvertently violated.

DEFENSE ADVANCED
RESEARCH PROJECTS AGENCY

Building Resource Adaptive Software Systems (BRASS)

Dr. Suresh Jagannathan

Modern-day software operates within a complex ecosystem of libraries, models, protocols and devices. Ecosystems change over time in response to new technologies or paradigms, as a consequence of repairing discovered vulnerabilities (security, logical, or performance-related), or because of varying resource availability and reconfiguration of the underlying execution platform. When these changes occur, applications may no longer work as expected because their assumptions on how the ecosystem should behave may have been inadvertently violated.

DEFENSE ADVANCED
RESEARCH PROJECTS AGENCY

Building Resource Adaptive Software Systems (BRASS)

Dr. Suresh Jagannathan

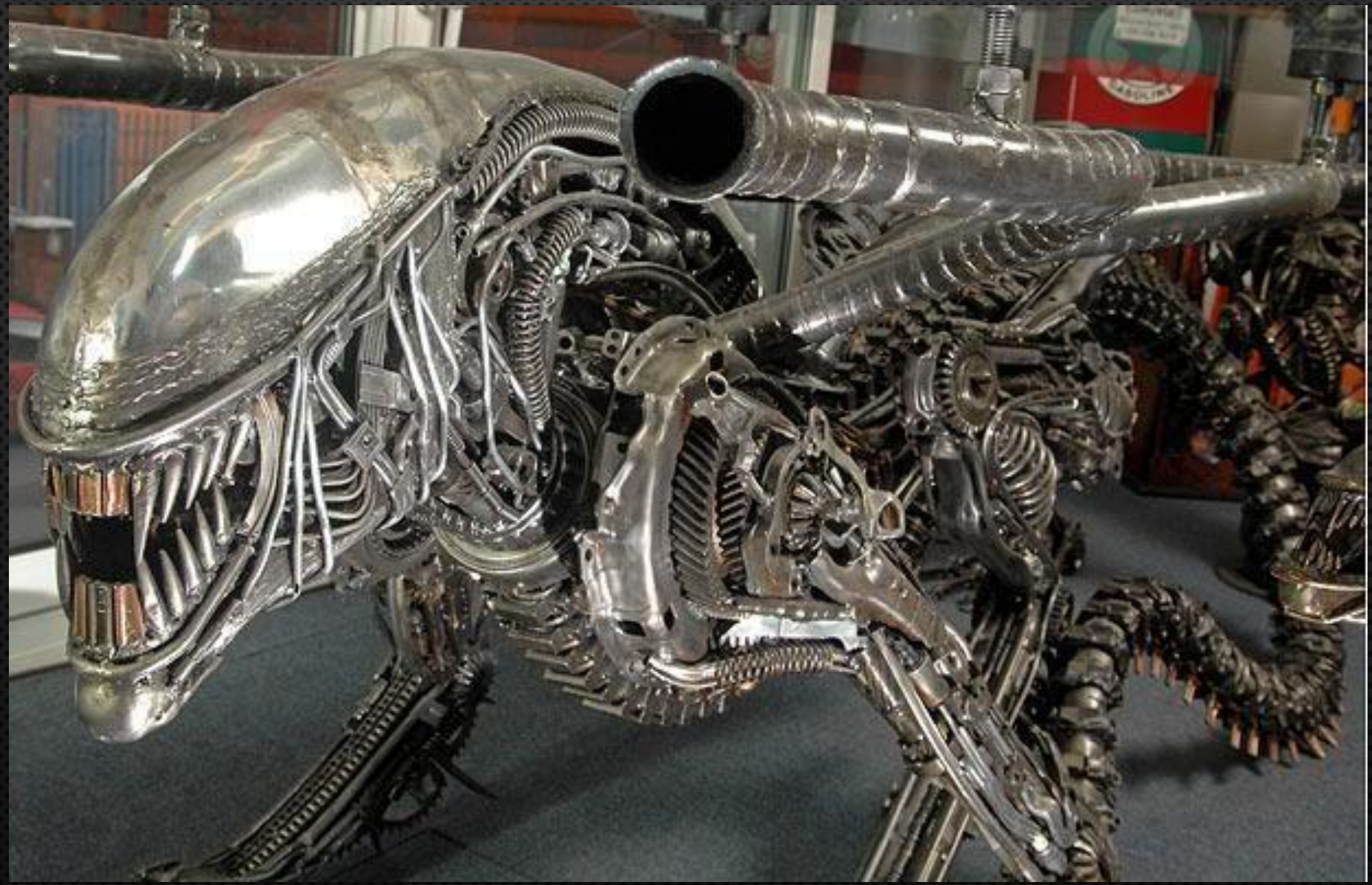
Modern-day software operates within a complex ecosystem of libraries, models, protocols and devices. Ecosystems change over time in response to new technologies or paradigms, as a consequence of repairing discovered vulnerabilities (security, logical, or performance-related), or because of varying resource availability and reconfiguration of the underlying execution platform. When these changes occur, applications may no longer work as expected because their assumptions on how the ecosystem should behave may have been inadvertently violated.

Successfully adapting applications to an evolving ecosystem requires mechanisms to infer the impact of such evolution on application behavior and performance, automatically trigger transformations that beneficially exploit these changes and provide validation that these transformations are correct.

1. Active Authentication
2. Active Cyber Defense (ACD)
3. Automated Program Analysis for Cybersecurity (APAC)
4. Behavioral Learning for Adaptive Electronic Warfare (BLADE)
5. Building Resource Adaptive Software Systems (BRASS)
6. Clean-slate design of Resilience, Adaptive, Secure Hosts (CRASH)
7. Computer Science Study Group (CSSG)
8. Crowd Sourced Formal Verification (CSFV)
9. Cyber Fault-tolerant Attack Recovery (CFAR)
10. Cyber Grand Challenge (CGC)
11. Dispersed Computing
12. Edge-Directed Cyber Technologies for Reliable Mission Communication (Edge CT)
13. Enhanced Attribution
14. Extreme DDoS Defense (XD3)
15. High-Assurance Cyber Military Systems (HACMS)
16. Integrated Cyber Analysis System (ICAS)
17. Leveraging the Analog Domain for Security (LADS)
18. Memex
19. Mission-oriented Resilient Clouds (MRC)
20. Plan X
21. Rapid Attack Detection, Isolation and Characterization Systems (RADICS)
22. Safeware
23. Space/Time Analysis for Cybersecurity (STAC)
24. Transparent Computing
25. Vetting Commodity IT Software and Firmware (VET)

BIOLOGY & ECOLOGY & NATURAL SYSTEMS

BIOLOGY & ECOLOGY & NATURAL SYSTEMS

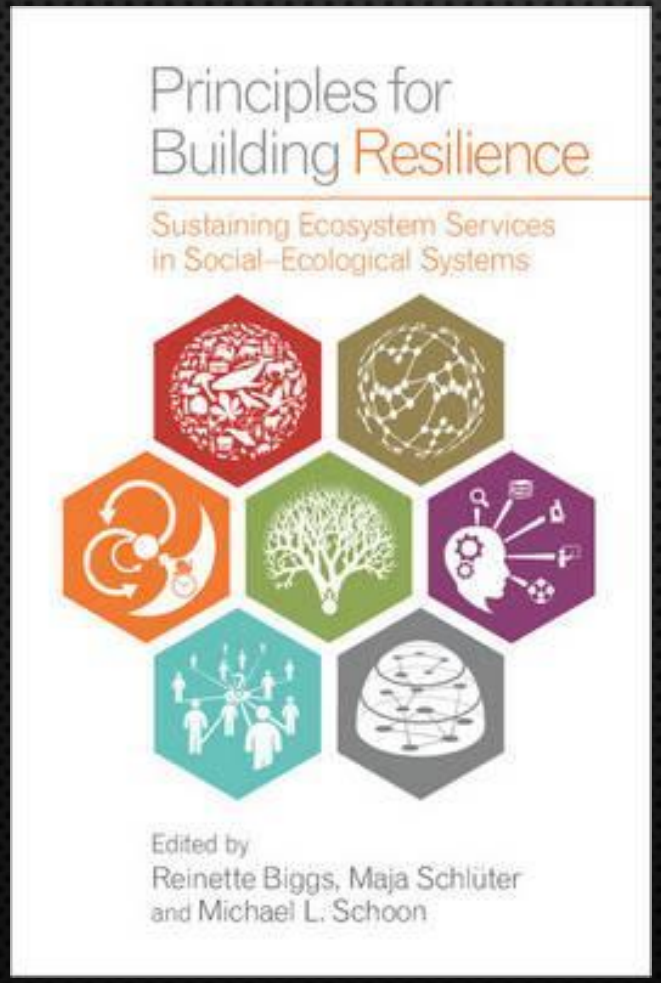


Applying resilience thinking

Seven principles for building resilience in social-ecological systems

Stockholm Resilience Centre

CAMBRIDGE UNIVERSITY PRESS



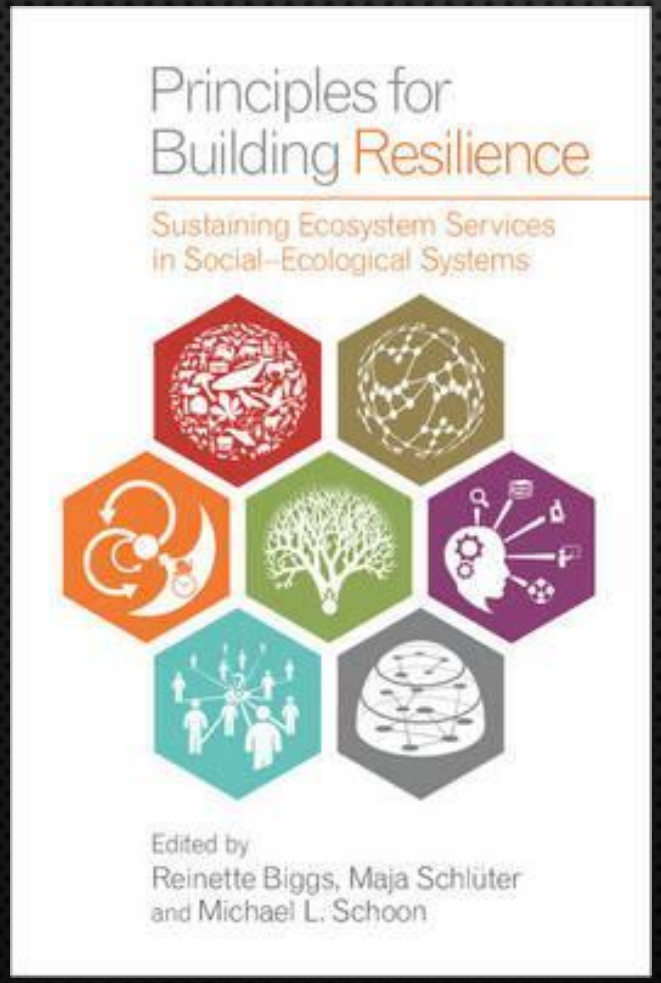
http://stockholmresilience.org/download/18.10119fc11455d3c557d6928/1459560241272/SRC+Applying+Resilience+final.pdf
& http://www.resalliance.org/news/19

Applying resilience thinking

Seven principles for building resilience in social-ecological systems

Stockholm Resilience Centre

CAMBRIDGE UNIVERSITY PRESS



1. MAINTAIN DIVERSITY AND REDUNDANCY
2. MANAGE CONNECTIVITY
3. MANAGE SLOW VARIABLES AND FEEDBACKS
4. FOSTER COMPLEX ADAPTIVE SYSTEMS THINKING
5. ENCOURAGE LEARNING
6. BROADEN PARTICIPATION
7. PROMOTE POLYCENTRIC GOVERNANCE SYSTEMS

http://stockholmresilience.org/download/18.10119fc11455d3c557d6928/1459560241272/SRC+Applying+Resilience+final.pdf
& http://www.resalliance.org/news/19

Principle one

Maintain diversity and redundancy

Principle one

Maintain diversity and redundancy

- Functional redundancy – multiple components can fulfill the same function
- Response diversity – components filling the same function respond differently to change/disturbance/attack

- Functional redundancy – multiple components can fulfill the same function
  - Dark net
  - Backups
  - Manual operations
- Response diversity – components filling the same function respond differently to change/disturbance/attack

Principle one

Maintain diversity and redundancy

- Functional redundancy – multiple components can fulfill the same function
  - Dark net
  - Backups
  - Manual operations
- Response diversity – components filling the same function respond differently to change/disturbance/attack
  - Utility networks are diverse and respond differently to attacks
  - Utilities manage cyber incidents differently

How do you balance:

Efficiency vs. Redundancy

Standardization vs. Diversity

Principle two

Manage connectivity

Principle two

Manage connectivity

- Inventory of devices & software
- Secure configurations
- Principle of Least Privilege – controlled use of Admin Privileges
- Logging & Monitoring
- Control of network ports, protocols, & Services
- Secure coding

Principle two

Manage connectivity

Complexity of systems

Principle two

Manage connectivity

Complexity of systems

Interdependencies not always known

Principle two

Manage connectivity

Complexity of systems

Interdependencies not always known

Tools – ease of use, false positives, etc.

Principle two

Manage connectivity

Complexity of systems

Interdependencies not always known

Tools – ease of use, false positives, etc.

Human in the Loop vs. Automation

Principle two

Manage connectivity

How do we reconnect compromised systems?

Is diversity a problem or a solution?
Standardized/modular systems

Patch / Change management

Principle three

Manage slow variables and feedbacks

Principle three

Manage slow variables and feedbacks

- Monitoring & anomaly detection – accounts, traffic, connections, etc.
- Incident response
- Information sharing
- Pen tests and red team assessments
- Honey pots, sandboxes, etc.

Principle three

Manage slow variables and feedbacks

Machine learning – slow intrusions

Principle three

Manage slow variables and feedbacks

Machine learning – slow intrusions

When do you let the intruder know you know?

Principle three

Manage slow variables and feedbacks

Machine learning – slow intrusions

When do you let the intruder know you know?

Detection – 2015 median =146 days (416 in 2012)

Principle three

Manage slow variables and feedbacks

Machine learning – slow intrusions

When do you let the intruder know you know?

Detection – 2015 median =146 days (416 in 2012)

Do we have 'canaries'?

Principle four

Foster complex adaptive systems thinking

Principle four

Foster complex adaptive systems thinking

- Dynamic
- Cause & effect separated in space and time
- Inherent uncertainty
- Produce adaptive and emergent structures, patterns, & behaviors
- Critical thresholds

Principle four

Foster complex adaptive systems thinking

- Dynamic
- Cause & effect separated in space and time
- Inherent uncertainty
- Produce adaptive and emergent structures, patterns, & behaviors
- Critical thresholds
- Non-linear changes
- Complex ≠ Complicated
- Continuous learning – build on emergent information
- Centralized Command & Control may not work

- Develop threat models – human behavior
- Systems thinking – analyzing independent data streams
- Personnel training, cross-disciplinary training

Principle four

Foster complex adaptive systems thinking

SCIENCE OF CYBER SECURITY – NOT WELL DEFINED

Principle four

Foster complex adaptive systems thinking

Science of Cyber Security – not well defined

Human behavior – attacker and attacked

Principle four

Foster complex adaptive systems thinking

Science of Cyber Security – not well defined

Human behavior – attacker and attacked

Mathematics, algorithms

Principle four

Foster complex adaptive systems thinking

Science of Cyber Security – not well defined

Human behavior – attacker and attacked

Mathematics, algorithms

Distributed decision making – Emergent shared response

Principle five

Encourage learning

Principle five

Encourage learning

MANAGEMENT

- Adaptive management – hypothesis, inquiry driven
- Adaptive co-management – including stakeholders in inquiry, sharing across silos
- Adaptive governance – matching the scale of the decision process to the scale of the cyber event, sharing across scales

Principle five

Encourage learning

MANAGEMENT

- Adaptive management – hypothesis, inquiry driven
- Adaptive co-management – including stakeholders in inquiry, sharing across silos
- Adaptive governance – matching the scale of the decision process to the scale of the cyber event, sharing across scales

LEARNING

- Single loop – how are we doing? Are we doing things right?

Principle five

Encourage learning

MANAGEMENT

- Adaptive management – hypothesis, inquiry driven
- Adaptive co-management – including stakeholders in inquiry, sharing across silos
- Adaptive governance – matching the scale of the decision process to the scale of the cyber event, sharing across scales

LEARNING

- Single loop – how are we doing? Are we doing things right?
- Double loop – are we doing the right thing?

Principle five

Encourage learning

MANAGEMENT

- Adaptive management – hypothesis, inquiry driven
- Adaptive co-management – including stakeholders in inquiry, sharing across silos
- Adaptive governance – matching the scale of the decision process to the scale of the cyber event, sharing across scales

LEARNING

- Single loop – how are we doing? Are we doing things right?
- Double loop – are we doing the right thing?
- Triple loop – do we know what the right thing to do is? Creating space for knowledge sharing across silos and scales

Principle five

Encourage learning

- Increasing skills and competencies within silos
- Cross training between IT, OT, Engineers, Software developers
- ES-C2M2 – self assessments across multiple job responsibilities

Principle five

Encourage learning

- Increasing skills and competencies within silos
- Cross training between IT, OT, Engineers, Software developers
- ES-C2M2 – self assessments across multiple job responsibilities
- Electricity Subsector Coordinating Council (ESCC)
- Electricity Information Sharing and Analysis Center (E-ISAC)
- Many!

Principle five

Encourage learning

Training curricula needed

Principle five

Encourage learning

Training curricula needed

Bringing stakeholders into inquiry process - trust

Principle five

Encourage learning

Training curricula needed

Bringing stakeholders into inquiry process - trust

Mismatches between scale of data collected and scale of impact – information sharing incomplete

Principle six

Broaden participation

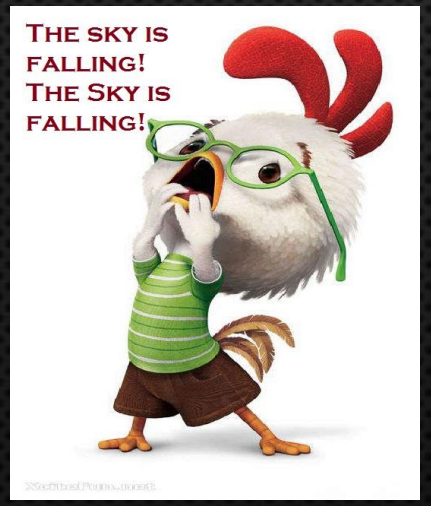
Principle six

Broaden participation

- Psychology of stewardship → Safety and Security
- Outreach to C-Suite
- Educational campaigns – cyber hygiene, National Cyber Security Awareness Month

Principle six

Broaden participation



SILOS STILL EXIST

BUSINESS CASE DIFFICULT

SKY IS FALLING ←→ THERE'S NOTHING WRONG

DIVERSE GOVERNANCE ENTITIES

Principle seven

Promote polycentric governance

Principle seven

Promote polycentric governance

Multiple interacting governance bodies with the autonomy to make and enforce rules – embedded in a horizontal or nested network

Principle seven

Promote polycentric governance

Multiple interacting governance bodies with the autonomy to make and enforce rules – embedded in a horizontal or nested network

- Electricity Subsector Coordinating Council (ESCC)
- Many!

Principle seven

Promote polycentric governance

Authority boundaries not always defined

Principle seven

Promote polycentric governance

Authority boundaries not always defined

Who bears the costs and who collects the benefits?

Principle seven

Promote polycentric governance

Authority boundaries not always defined

Who bears the costs and who collects the benefits?

Compliance vs. Security

Principle seven

Promote polycentric governance

Authority boundaries not always defined

Who bears the costs and who collects the benefits?

Compliance vs. Security

Does management of a cyber incident on one scale impact other scales?

BIOLOGY / ECOLOGY / NATURAL SYSTEMS RESILIENCE

CYBER RESILIENCE

Building Resilience

1. Maintain diversity and redundancy
2. Manage connectivity
3. Manage slow variables and feedbacks
4. Foster complex adaptive systems thinking
5. Encourage learning
6. Broaden participation
7. Promote polycentric governance systems

All hands on deck

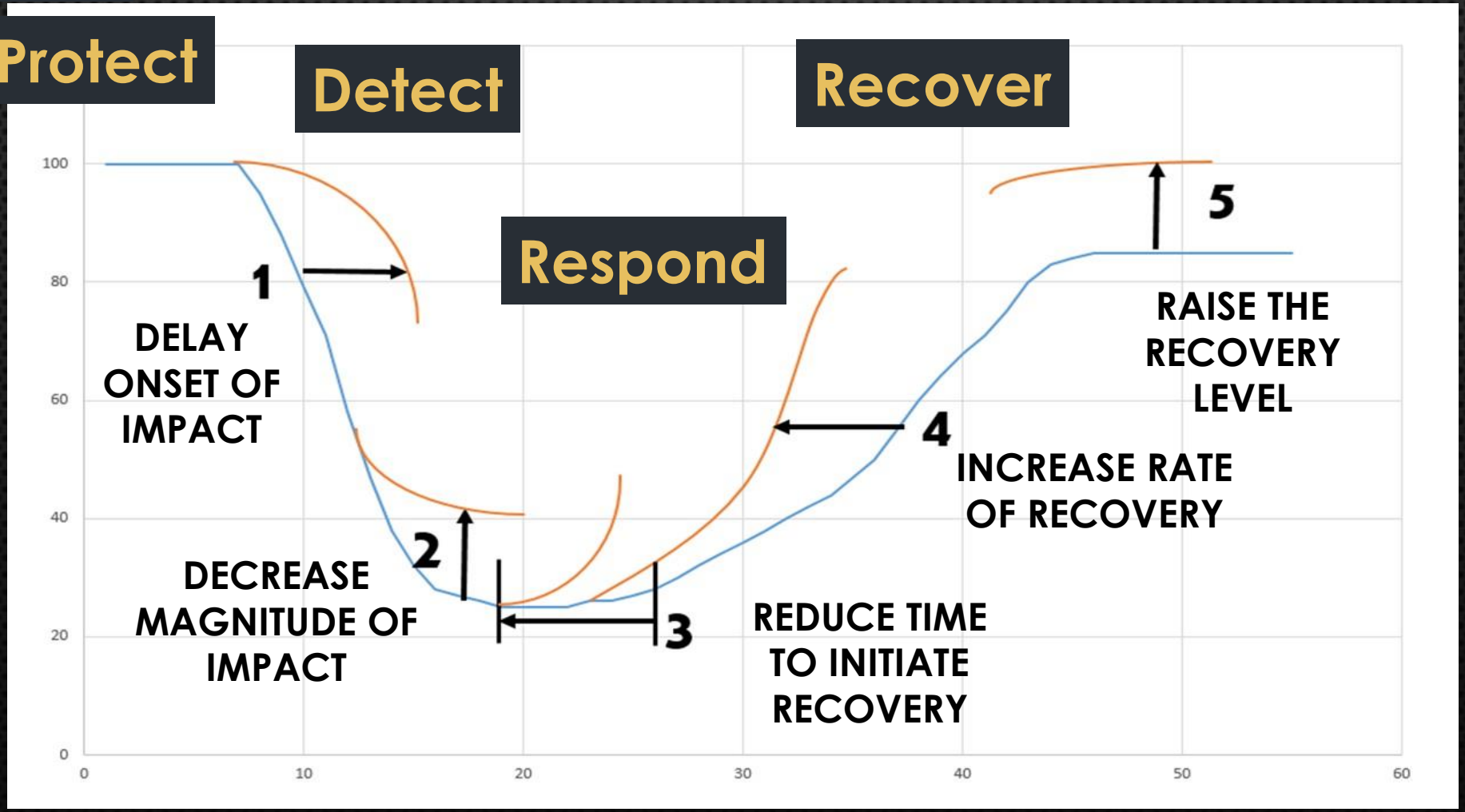
Identify

Protect

Detect

Recover

Respond



IT'S A DOG EAT DOG WORLD OUT THERE

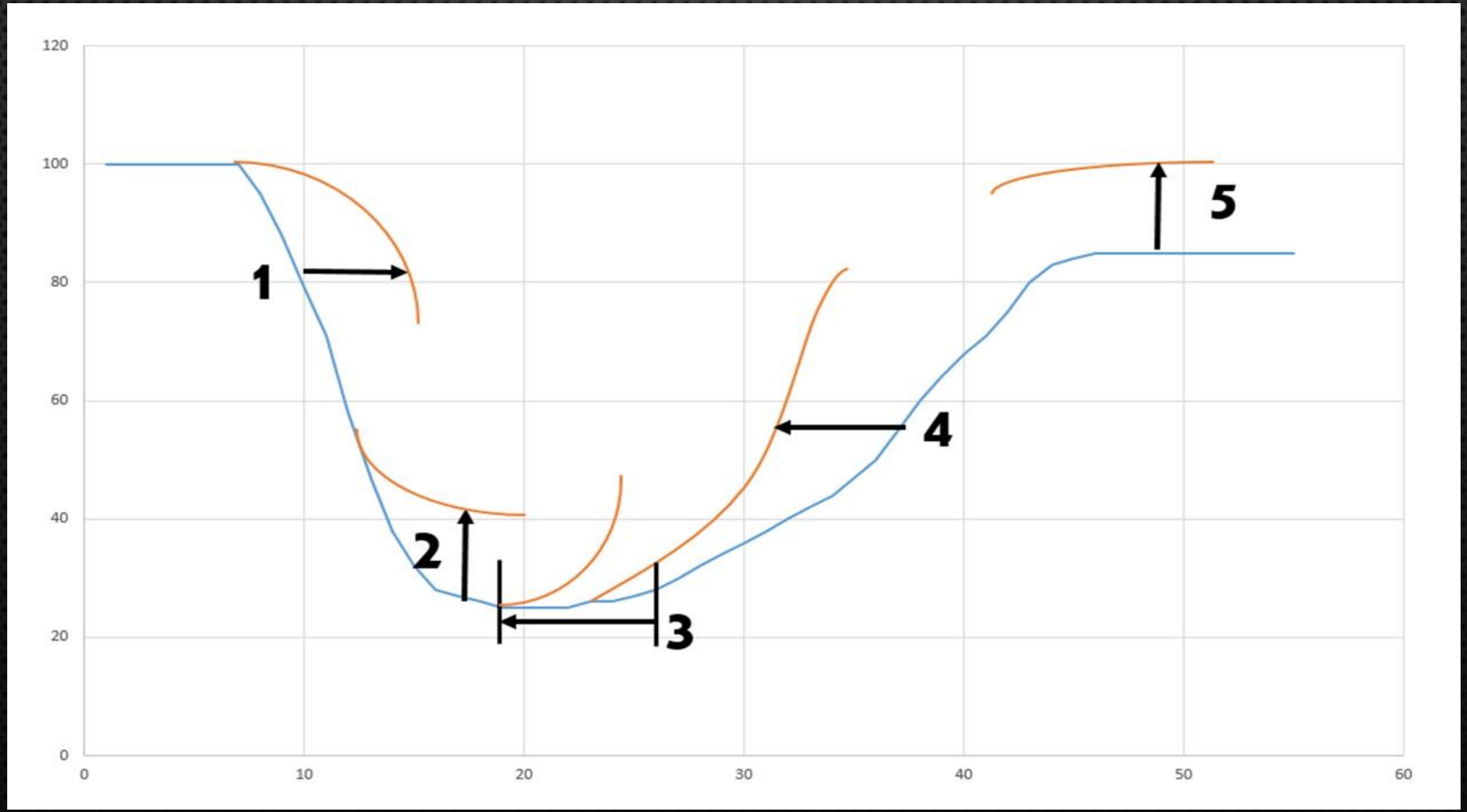
The Resilient Design Principles

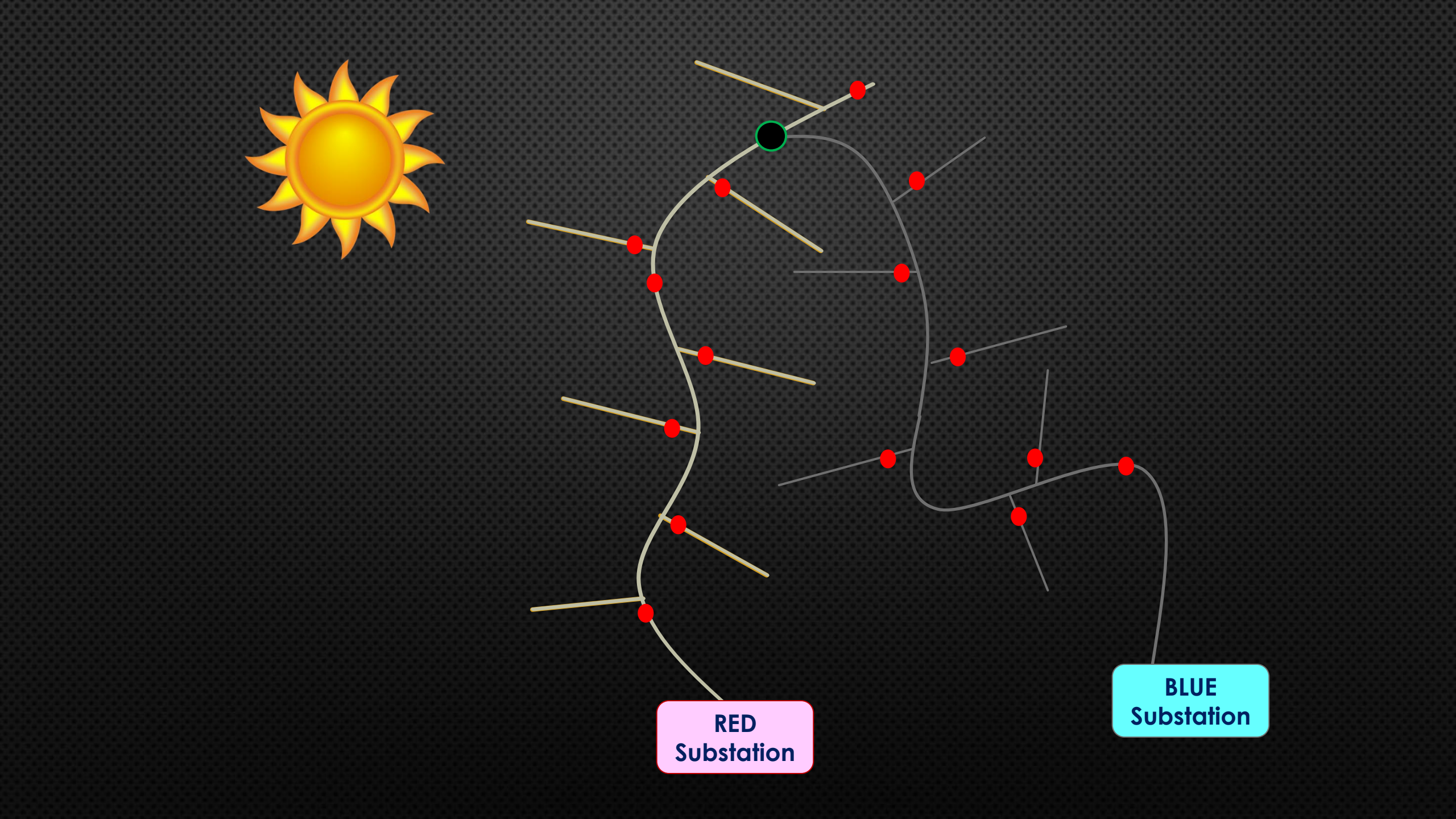
1. Resilience transcends scales
2. Resilient systems provide for basic human needs
3. Diverse and redundant systems are inherently more resilient
4. Simple, passive, and flexible systems are more resilient
5. Durability strengthens resilience
6. Locally available, renewable, or reclaimed resources are more resilient
7. Resilience anticipates interruptions and a dynamic future
8. Find and promote resilience in nature
9. Social equity and community contribute to resilience
10. Resilience is not absolute

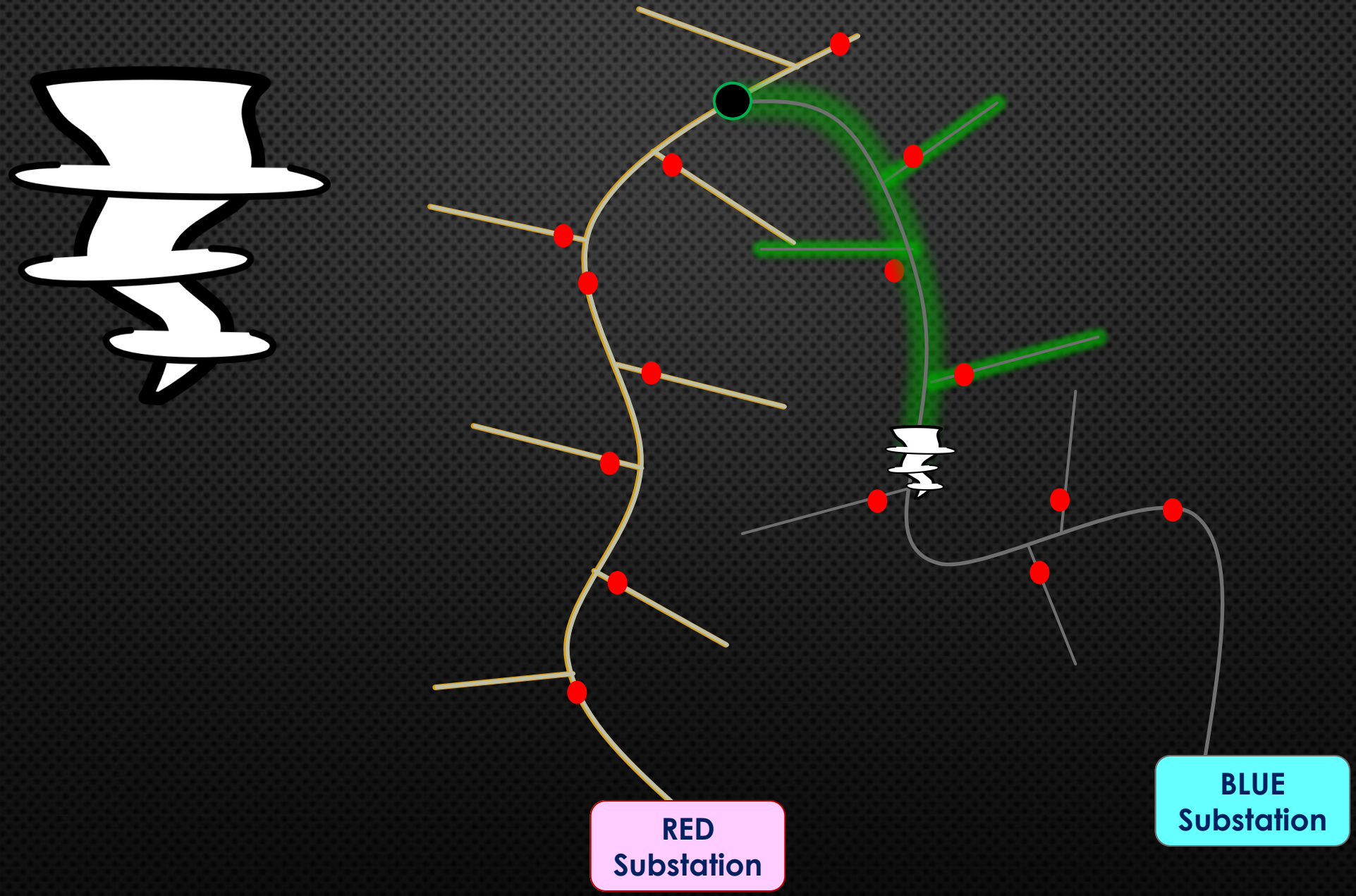
RESILIENT DESIGN INSTITUTE

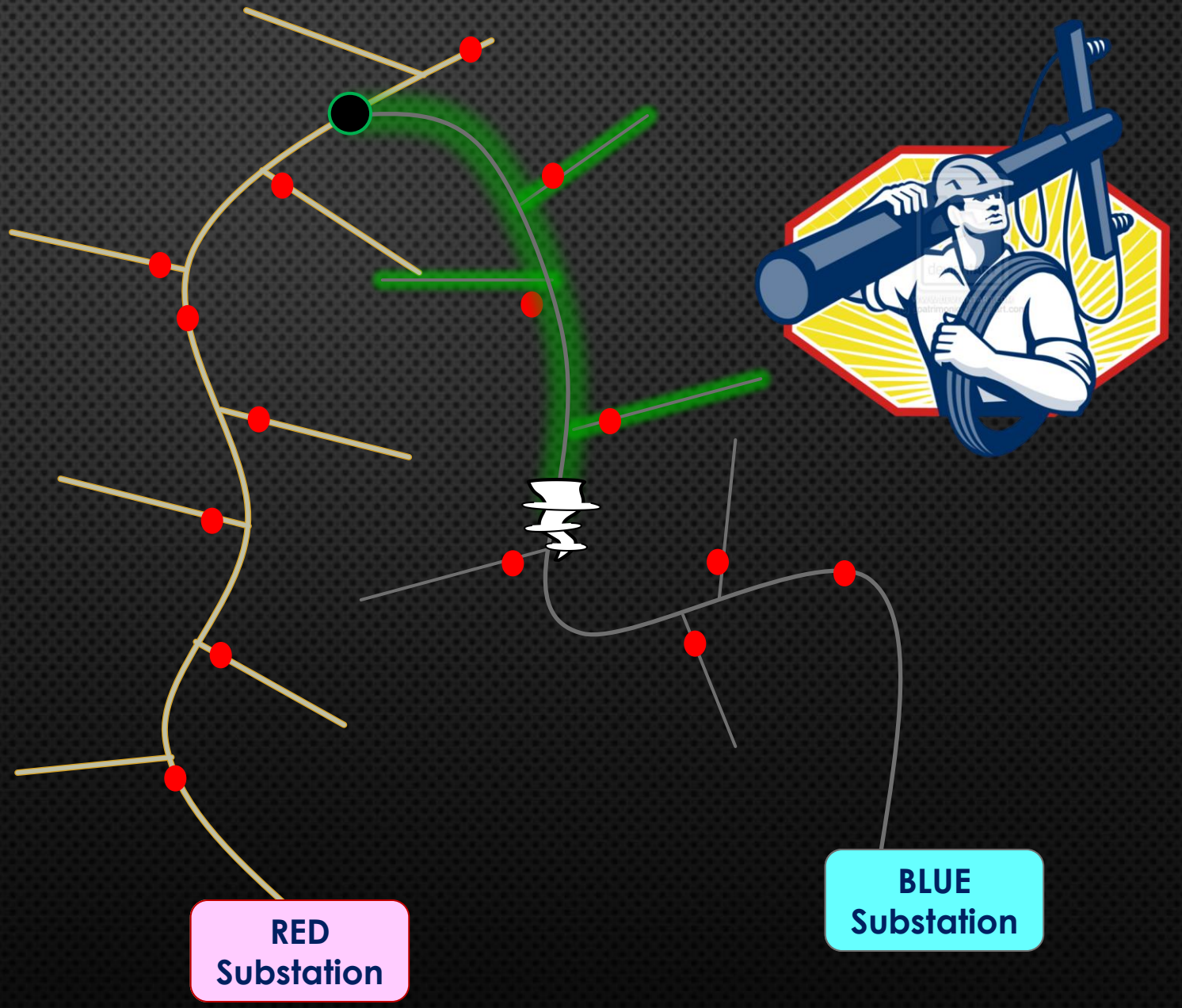
http://www.resilientdesign.org/the-resilient-design-principles/

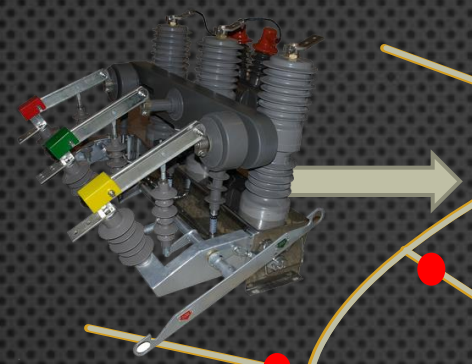
CAN THIS MODEL BE APPLIED TO CYBER?




RED
Substation
BLUE
Substation


RED
Substation
BLUE
Substation


RED
Substation
BLUE
Substation



RED
Substation

BLUE
Substation

BUT WHAT IF SIMPLE BACK FEEDING IS NOT ENOUGH?

RESILIENCY FROM

Advanced Sensor Technology + **Advanced Forecasting** + **Advanced Analytics** + **Advanced Control**

APPLY ALL "SMART GRID TECHNOLOGIES" IN A COORDINATED WAY

- SMART FEEDER SWITCHING
- ADVANCED SECTIONALIZATION
- ROLLING DISCONNECTS (DOWN TO METER LEVEL)
- DISPATCHABLE BACKUP GENERATORS
- DISTRIBUTED ENERGY
- ADVANCED VOLT/VAR CONTROL
- STORAGE
- …

Evolution in Grid Control

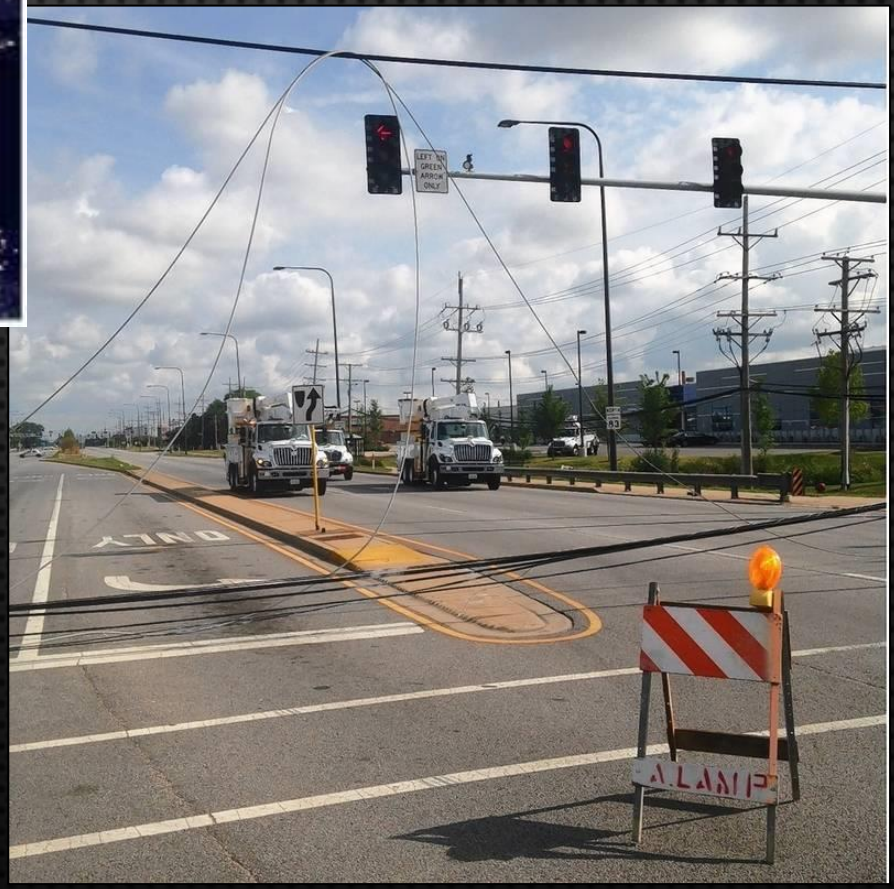
Historical Control Paradigm

- Hierarchical central control

The Agile / Fractal Grid

- Control areas are defined dynamically
- Autonomous (greedy) operation
- Collaborative operation
- Directed operation

RESILIENCY ≠ RELIABILITY



RESILIENCY vs RELIABILITY

Resiliency	Reliability
More local	Larger scale
Shorter duration	Longer duration
Limited economic impact	Large economic impact
Can be managed by utility	Requires societal level coordination
Established Metrics	Metrics still to be defined